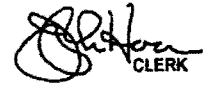


UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

FILED

JAN 31 2014


CLERK

IN THE MATTER OF THE SEARCH OF:

The premises known as the offices of
Google Inc., 1600 Amphitheatre
Parkway, Mountain View, CA 94043
Account: cgodfrey4285@gmail.com

14-mc-05

STATE OF SOUTH DAKOTA)	Affidavit in Support of
)	Application for Search Warrant
COUNTY OF PENNINGTON)	

I, Jonathan Kirk, am employed as an Investigator with the Pennington County Sheriff's Office. I began my law enforcement career in December of 2005 with the Pennington County Sheriff's Office. During my employment with the Pennington County Sheriff's Office, I was assigned as a Patrol Deputy where I responded to and investigated assaults, sexual assaults, child abuse cases, and domestic violence issues. In September of 2008, I was assigned as an investigator in the Investigations Division. My primary duties are the investigation of sex crime and internet crimes such as Solicitation of Minors, Sexual Exploitation of Minors, Child Pornography, and Rape. During my career, I have been involved in the investigation of numerous crimes including homicide, rape, child abuse, child pornography, theft, and burglary. During my career, I have received over 600 hours of informal and formal training. My training is primarily from the South Dakota Law Enforcement Academy and Pennington County Sheriff's Office. Additionally, I have attended training courses as a Field Training Instructor, Taser Instructor, Peer to Peer Computer Investigations,

Undercover Peer to Peer Investigations (Gnutella, Ares, BitTorrent Networks), ICAC (Internet Crimes Against Children) Investigative Techniques, ICAC Undercover Chat Training, Advanced Responders: Search and Seizure of Networks, Cell Phone and Portable Storage Forensics, and Interview and Interrogation Training.

1. I make this affidavit in support of an application for a search warrant for a certain account controlled by the email service provider known as Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, CA, 94043. The account to be searched is cgodfrey4285@gmail.com, which is further described in the following paragraphs.

2. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for a warrant pursuant to 18 U.S.C § 2703 to search a specific Google, Inc. (Gmail) account (identified herein as the "Target Account"), I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information contained in this Affidavit is based upon my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance, and in part only.

3. I have spoken to other agents, law enforcement officials, and other interested individuals about this investigation, and have read reports concerning the progress of the investigation. The statements contained in this affidavit are based on information that has been provided to me directly or

indirectly by witnesses, other law enforcement officers, and agents. The information and conclusions expressed are also based upon my own experience and training as a law enforcement officer, and my personal involvement and knowledge gained during the course of this investigation.

BACKGROUND REGARDING COMPUTERS, THE INTERNET AND E-MAIL

4. Based on my training and experience, I know the following:
 - a. The internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. The term "computer" as used herein is defined in 18 U.S.C § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;
 - b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods;
 - c. A computer on the Internet is most commonly identified by an Internet Protocol Address ("IP address"), which is usually traceable back to a particular Internet service provider ("ISP") that provides the user with an internet connection. One can easily determine the ISP to which these IP addresses are registered using publically available databases. ISPs often log which individual customers are assigned IP addresses at a given date and time, both for billing and technical support reasons. However, ISPs often retain information allowing them to identify the subscriber assigned a particular IP address for only a very short time. As a practical matter, by the time one has gleaned the IP address that accessed an account from materials produced in compliance with an order under 18 U.S.C § 2703(d), the ISP in

question can often no longer determine which of their subscribers had the IP address on that date and time in question. Often, to positively identify an individual connecting over a particular IP address, some form of real-time monitoring will be required; and

- d. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

Based on my training and experience and investigation in this case, I have learned the following about Google:

- a. Google offers an e-mail service that is available free to Internet users called "Gmail". Stored electronic communications, including opened and unopened e-mail for Gmail subscribers may be located on Google's computers.
- b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.
- c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.
- d. Any e-mail that is sent to a Gmail e-mail subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.

- e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, where they are retained until deleted or the storage limit is exceeded.
- f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e-mail.

6. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Accounts specified herein and in Attachment A, following the procedures described herein.

**AUTHORITY TO ACCESS CONTENT OF ELECTRONIC COMMUNICATIONS
AND TRANSACTIONAL DATA AND SUBSCRIBER INFORMATION**

7. *Stored Communications.* Pursuant to 18 U.S.C. §§ 2703(a) and (b), if the government obtains a search warrant issued under the Federal Rules of Criminal Procedure, it can require a provider of electronic communication service to disclose the contents of a

subscriber's stored wire or other electronic communication, without giving notice to that subscriber.

8. Transactional (Non-Content) Data. Pursuant to 18 U.S.C. 2703(c)(1)(A), the government also has the authority to access non-content, transactional data that an Internet provider retains about its subscribers. Such transactional information might include the To: or From: lines on paste-mail messages, the Internet Protocol ("IP") numbers used to route these messages over the Internet; log files showing dates, times, and methods of connecting to Google's computers; other Internet locations to/from which a subscriber came or went; purchases made; the number of visitors or "hits" a subscriber's web page has received, and services accessed through a subscriber's personalized "home" or "Gmail" web pages. The government may access such non-content, transactional data using "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure..."

9. Subscriber Information. Pursuant to 18 U.S.C. § 2703(c) (2), the government may also obtain the following subscriber information from a service provider:

- a. Name;
- b. Address;
- c. Local and long distance telephone connection records, or records of session times and durations;
- d. Length of service (including start date) and types of service utilized;

- e. Telephone or instrument number or other subscriber number or identity including any temporarily assigned network address such as an Internet Protocol Address;
- f. Means and source of payment for such service (including any credit card or bank account number).

10. *The Authority of this Court.* A warrant for disclosure of the e-mail contents, transactional data, or subscriber records may be issued by any "court of competent jurisdiction over the offense under investigation." See 18 U.S.C. §§ 2711(3) (A) (i), 2703(a), 2703(b) (1) (B), 2703(c) (l) (A), and 2703(d). Thus, a search warrant may be issued by a federal magistrate in this district, even if the electronic records sought by the government reside in another district. See United States v. Freeman, 2010 WL 4386897 (D. Minn. 2010) (The statutory language of 18 U.S.C. § 2703 "specifically authorizes the issuance of [search warrants for electronic communications and evidence to be executed out of the district].")

11. *Method of Service.* If this Court issues a warrant as requested by the government, a law enforcement officer need not be present to serve or execute that warrant upon Google, pursuant to 18 U.S.C. § 2703(g), which provides:

"Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service."

Thus, a search and seizure of electronic data from Google's server by Google's technicians has been viewed as reasonable under the Fourth Amendment in the Eighth Circuit. See *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002).

PROBABLE CAUSE

12. On 01-16-14 Special Agent Brent Gromer received a telephone call from Sgt. Eric Jones, Nebraska State Patrol. Sgt. Jones advised S/A Gromer that his agency was currently investigating an individual who stated that he worked as a custodian at a Rapid City Elementary School. Sgt. Jones advised S/A Gromer that Trooper Monty Lovelace had been conducting undercover chats with this individual posing as a 14 year old girl. During those chats, Sgt. Jones informed S/A Gromer the individual had asked for photos of the "14 year old girl" and sent a photo of his penis.

13. On 01-16-14 S/A Gromer spoke with Trp. Lovelace who relayed the same information about his contacts with the unknown individual. Trp. Lovelace advised that during his undercover chat with this individual the person told him that he worked as a custodian at a local Rapid City School. The individual also informed Trp. Lovelace that he "really liked" a teacher at the school and provided the name "Averie". He stated he also really likes an 11 year old student at the school named "Patience". S/A Gromer made contact with Det. Wayne Keefe, Rapid City Police Department, with the information received from Trp. Lovelace in an attempt to identify the individual. Det. Keefe was able to find that Pinedale

Elementary employed a 4th grade teacher, Averie Georgas, and had an 11 year old student, Patience Sunstrom, at the school. Det. Keefe also identified a Custodian at the School, Casey Godfrey. Det. Keefe received a driver's license photo for Casey Godfrey which matched the photo Trp. Lovelace had received from the person with whom he was chatting.

14. On 01-16-14, Trp. Lovelace forwarded copies of his undercover chat to S/A Gromer and I. Trp. Lovelace was using an undercover identity and Godfrey was using the screen name "boneman4285". I reviewed those chats. I noticed the undercover agent told Godfrey they were 14 years old. I also found Godfrey had requested pictures multiple times from the undercover agent. Godfrey specifically asked for "other" pictures on 01-15-14 at 08:24:04 AM. Godfrey then asked for "naughty ones" after that. At 08:43:11 AM, on 01-15-14, Godfrey sends the following message: "you show me yours, I'll show you mine when you get out of school".

15. In the afternoon of 01-16-14, Godfrey begins asking the undercover agent for panty pictures. Godfrey also sent the following message at 01:30:24 PM "ok, I'd like to see some from the shower too if that's cool".

16. During their conversation, the undercover sent a picture of a fold in the skin of his arm to Godfrey. The undercover portrayed it as a picture of their vagina. Godfrey later sent the undercover a picture of an adult male's penis. A white ring can be seen on the subject's hand, which is holding onto the penis. Godfrey claims the picture is of his penis.

17. On 01-16-14, at approximately 1406 hours, Det. Wayne Keefe and I contacted Godfrey at Pinedale Elementary. Godfrey was walking away from a custodian office area. I identified myself to Godfrey and explained why were there. Godfrey said his cell phone was in the back office area. I then located an AT&T HTC cell phone (S/N HT19XT211135) sitting on top of a work desktop, which was currently on and running. I asked Godfrey if the cell phone was his and he indicated it was. I noticed the computer had an open internet page open to the Yahoo email of "boneman4285". The full email account was later determined to be: boneman4285@yahoo.com Det. Keefe took pictures of the screen and we seized the desktop computer and Godfrey's cell phone for evidentiary purposes.

18. When dealing with Godfrey, I noticed a white wedding band on his left ring finger. This appeared to match the ring seen in the picture sent by Godfrey.

19. Det. Keefe and S/A Gromer met with Godfrey's wife, Megan Godfrey, at her place of employment on 01-16-14. Megan reported that Godfrey uses their home computer and iPad for ½ hour a day before she returns home from work.

20. The undercover officer has also spoken with Godfrey on the internet site Motherless.com.

21. A search warrant was applied for and granted for Godfrey's cell phone and his residence. During a search of Godfrey's cell phone content, another email account used by Godfrey was located as part of the email section on the phone. The email account was that of: cgodfrey4285@gmail.com. The

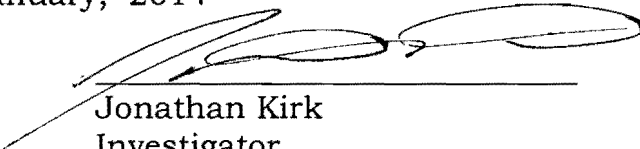
email content appeared to be communication between Godfrey and other individuals about having sex or meeting for sex.

CONCLUSION

22. Based upon the information above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, there exists evidence, fruits, and instrumentalities of violations of, 18 U.S.C. §§ 2422(b) and 1470. By this Affidavit and application, I respectfully request that the Court issue a search warrant under 18 U.S.C. § 2703 directed to Google, allowing agents to seize the electronic communications and other information stored on the Google servers for the computer accounts and files described in Attachment A.

23. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. by facsimile and to allow Google, Inc. to copy the data outside of this officer's presence.

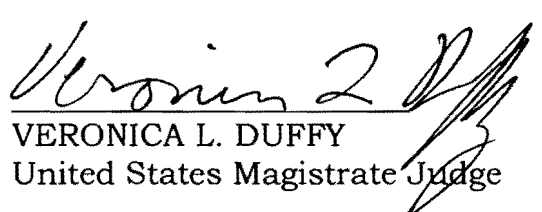
Dated this 3/5th day of January, 2014



Jonathan Kirk
Investigator
Pennington County Sheriff's Office

Sworn to before me and subscribed in my presence,

1-31-14
Date



VERONICA L. DUFFY
United States Magistrate Judge